NASA SBIR 2022 Phase I Solicitation

A2.04 AERONAUTICAL INFORMATION SYSTEM SECURITY (AISS): Aircraft Systems

Lead Center: GRC

Scope Title

Onboard Noninvasive Intrusion Detection Systems

Scope Description

To accommodate the anticipated diversity and complexity of operations in the future National Airspace System (NAS), the system must be more digitally connected, but by being connected this provides more pathways for hackers into the NAS and its systems, increasing the likelihood that an aircraft will be hacked. With new entrants, such as Unmanned Aircraft Systems (UAS) and Advanced Air Mobility (AAM), they will rely on third party services to operate. There is a need to detect safety events and safety threats caused by hackers to increase the abilityÂ of the systemwide safety assurance to perform its functions.Â The increased assurance will play a critical role in how quickly new operations and new vehicles can be safely integrated with NAS operations. NASA is developing ground and vehicle based In-Time System-Wide Safety Assurance (ISSA) capabilities to monitor, assess and mitigate safety threats, and this SBIR will address the detection of cybersecurity threats that will cause safety threats, to both commercial and emerging operations. The eventual goal is for these capabilities to be integrated into an In-Time Aviation Safety Management System (IASMS) capable of system-level safety assessment.

This subtopic seeks technologies to enhance cybersecurity monitoring and assessment capabilities for air-vehicle-based systems. This may include cyber related ISSA tools or techniques that fit within the architecture being developed by NASA or it may include a separate cybersecurity device that performs monitor-assessÂ functions whose outputs may be integrated with a larger IASMS at some future point. Proposal areas include, design architectures, and development and/or demonstration in the following areas, with an emphasis on onboard flight cyber safety:

- Onboard system monitoring and assessingÂ with reporting both locally and to off-board operations centers.
- Interfacing to the larger network systems monitoring and assessingÂ with reporting, both locally and to operations centers.
- Integration of individual monitor-assessingÂ instances into the greater system-of-systemÂ approach, either standalone or as a capability of safety ISSA architectures.

From a functionality point of view, each instance of the monitor-predict entity, a combination of entities, or the systemwide ISSA may perform one or more of these functions:

- Monitor: detect anomalies or deviations from normal operations.
- Assess:Â localization;Â determine attack target, provide analysis to forecast the probability of events.

- Report: onboard, off board, and logging.
- Mitigate: when mitigation is possible, mitigate incidents without loss of operational and prioritize corrective actions for onboard operators/systems.

Given the developing Advanced Air Mobility (AAM)Â and traditional aviation systems, several possible analytical approaches may be possible.Â These include:

- Digital Twin:Â analytical combinations of on onboard and off-board models.
- Attestation:Â provable by observation methodologies.
- Traffic monitoring:Â monitoring of aviation bus data, network data, or other data flows.
- MDAO:Â multidisciplinary design analysis optimization.
- Artificial intelligence/machine learning:Â i.e., â€œteachâ€ a model to adapt itself to defenses as they engage.

Expected TRL or TRL Range at completion of the Project

2 to 5

Primary Technology Taxonomy

Level 1

TX 08 Sensors and Instruments

Level 2

TX 08.3 In-Situ Instruments/Sensor

Desired Deliverables of Phase I and Phase II

- Â HardwareÂ
- Â SoftwareÂ
- Â AnalysisÂ
- Â PrototypeÂ
- Â Research

Desired Deliverables Description

Phase I:

- Analysis and architectures for onboard cyber anomaly monitoring system, to include aviation buses and other data flows.
- Analysis and architectures for predictive analysis of cyber anomalies.
- Reporting capabilities to operations centers.

Phase II:

- Analysis and architectures for systemwide cyber anomaly monitoring including node and aggregation methods.
- Mitigation: analysis and design of cyber-resilience methodologies that include mitigation incidents without loss of mission success.
- Prioritize corrective actions for operators/systems.
- Propose a demonstration system implementation including hardware, software, testing, and validation.

State of the Art and Critical Gaps

There are clear limitations to near term adoption of these new cyber technologies into the National Airspace System (NAS) or the AAM equivalent.Â These include:

- Current aviation communication technologies, certified for use in the NAS, are severely limited in bandwidth and constrained to specific functions.Â This makes concepts that may move large amounts of data between air vehicles and the ground difficult to implement.
- In-time data prediction can be computer processing unitÂ (CPU) intensive.Â The onboard capabilities of Unmanned Aircraft Systems (UAS) and AAM-type vehicles may not provide significant onboard processing capabilities.
- Data needed for the prediction of aviation cyber events is not well understood or data is difficult to obtain or synthesize.
- Data needed for aviation cybersecurity machine learning methodologies is also difficult to obtain and validate.Â Attempts to use information technology (IT) ground-based systems as surrogates for aviation systems may not yield reliable comparisons.

Relevance / Science Traceability

As our world becomes more digitally connected, there are increasing opportunities for cyber-attacks across all domains. Aviation is no exception.

Communication links and maintenance loads are susceptible to viruses and other attacks. Most communication systems in the aircraft are not protected via authentication or by encryption and with newer systems that rely on commercial standards like Ethernet and Internet Protocols (IP) vulnerability to cyber threats increases. It is possible to send data to an aircraft via the communications link and if the messages are formatted properly, they will be acted up by the onboard systems, potentially causing Denial of Service attack or affecting other systems by disrupting processes. This SBIR focuses on air vehicle cybersecurity and seeks proposals for observation of nominal system states, assessment and reporting of off-nominal traffic, and mitigation of off-nominal operations.
Â Â

References

Eurocae / RTCA Aeronautical Information Systems Security (AISS), Airworthiness Security Methods and Considerations, Information Security Guidance for Continuing Airworthiness,Â Process Standard for Security Certification and Declaration of ATM ANS Ground Systems and Guidance on Security Event Management.Â

Ellis, K., Koelling, J. Davies, M, Krois, P. (2020)Â In-time System-wide Safety Assurance (ISSA) Concept of Operations and Design Considerations for Urban Air Mobility (UAM),Â NASA/TMâ€”2020â€“5003981

Â